Release Notes for BayRS Version 13.10

BayRS Version 13.10
Site Manager Software Version 7.10
BCC Version 4.10

Part No. 301151-C Rev 00
November 1998

Bay Networks *Where Information Flows.*™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. November 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

AN, BCN, BLN, BN, FRE, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BayStack, SPEX, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Bay Networks Technical Publications xi
How to Get Help xii

Release Notes for BayRS Version 13.10

Year 2000 Compliance 2
Upgrading to Version 13.10 2
Upgrading ATM Configurations 2
Upgrading L2TP Configurations 3
Upgrading OSPF Configurations 3
Upgrading the BCC Help File 3
Event Database 4
Quick2Config 4
SunOS 4.1.4 Support for Site Manager 5
Using the BCC 5
Platforms Supported 5
Number of BCC Sessions 5
BCC Help Initialization 6
Interfaces Supported 6
Global Protocols Supported 7
Interface Protocols Supported 7
Getting Started 8
Deleting Interfaces with the BCC 8
BCC show Command Documentation 9
Identifying Board Types 11
Sending BCC Feedback 17
New Features in BayRS Version 13.10 18
BaySecure FireWall-1 18

Backup Management Station Selection 18
BCC show config Options 20
BCC Support for Dial-on-Demand Service 20
BGP Configuration 21
Route Flap Dampening 21
Configuring EBGP for Route and Traffic-Load Balancing 21
Data Compression Enhancements 22
DHCP Server 22
DLSw PU Type 4 Device Support 22
Domain Name Server (DNS) Proxy 23
Generic Routing Encapsulation 23
HTTP Server 23
Improved Security 23
Domain Name Access 24
HTTP Server Parameters 24
IP Multicasting Configuration 24
DVMRP BCC Support 24
DVMRP Policies 24
IGMP Relay 25
IP Security (IPsec) 25
L2TP Support (RFC 1877) 26
Multiuser Access Control 27
Multiprotocol Label Switching (MPLS) 27
Protocol Statistics for MPLS 27
MPLS Routing Support 28
MPOA Enhancements 28
PVC Operations and Management 29
Syslog Support 29
Virtual Router Redundancy Protocol (VRRP) 29
WEP over Dial Services 29
New Hardware for BayRS 13.10 30
ARN E7S Support 30
BCC Support for the FRE2-060E Processor Module with Advanced Compression Coprocessor 30
BCC Support for the FRE-2-060E Processor Module 30

Support for 64 MB ATM Routing Engine 30
Guidelines for Working with BayRS Version 13.10 31
Amendment to Configuring PPP Services 31
AN/ANH and ARN Guidelines 31
Allocating Memory on ARN Routers 31
DSU/CSU Test LED Remains On After Reset 32
Network Booting on DSU/CSU Interfaces 32
ARN Router Not a Supported DVS RADIUS Client 32
BayRS Version 13.10 Flash Memory Requirements 32
Configuring PU 4 and SDLC Link Stations 32
Creating Multiple GRE Tunnels 33
FireWall-1 Redundant Management Scripts 33
Preparing and Transferring Firewall Files Between Windows NT Platforms 34
IP Fragmentation Not Supported over GRE Tunnels 34
IP Security (IPsec) Executable 34
Adding the IPsec File to the BayRS 13.10 Base Kernel 34
Multiuser Access 35
Sharing BCC Multiuser Access Profiles 35
BCC Lock Messages 35
Password Command 37
NAT Anomalies 37
Configuring NAT Dynamically 37
Deleting NAT from a Router 37
Outbound LAN Traffic Filters 38
Protocol Prioritization No Call Filters and TCP Applications 38
Support for Strata-Flash Card 38
WEP Executable 38
X.25 PVCs 39
Operating Limitations 39
Restriction When Deleting ATM from a Router if Signaling Is Enabled 39
Restriction if Signal Ports Settings on a Switch and Router Conflict 39
Restriction When Creating FTP from the BCC 39
Restriction When Deleting a Hybrid Mode Permanent Virtual Circuit (PVC) 40
Restriction When Using DLSw/APPN Boundary Port with AS400s and Other Adjacent Link Stations 40

Restriction When Virtual Channel Connections (VCCs) Become Inactive 40
Protocols Supported 40
Standards Supported 43
Flash Memory Cards Supported 48

Tables

Table 1. BCC Board Types: AN and ANH Modules 11
Table 2. BCC Board Types: BLN and BCN Modules 13
Table 3. BCC Board Types: ASN Modules 15
Table 4. BCC Board Types: ARN Modules 16
Table 5. BCC Board Types: System 5000 Modules 17
Table 6. 64 MB ATM Routing Engine Specifications 30
Table 7. Standards Supported by Version 13.10 43
Table 8. Approved Flash Memory Cards 48

Preface

BayRS Version 13.10 is a major software release that includes new features, functionality, and significant software changes made since BayRS Version 13.01. These release notes contain guidelines for using BayRS Version 13.10

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, information about educational services, and the telephone numbers of our global support offices, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

In the United States and Canada, you can dial 800-2LANWAN for assistance.

Release Notes for BayRS Version 13.10

This document contains the latest information about Bay Networks® BayRS™ Version 13.10.

These release notes include information about:

- Year 2000 Compliance
- Upgrading to Version 13.10
- Event Database
- Quick2Config
- SunOS 4.1.4 Support for Site Manager
- Using the BCC
- New Features in BayRS Version 13.10
- New Hardware for BayRS 13.10
- Guidelines for Working with BayRS Version 13.10
- Operating Limitations
- Protocols Supported
- Standards Supported
- Flash Memory Cards Supported

Year 2000 Compliance

BayRS Version 13.10 and Site Manager Software Version 7.10 are Year 2000 Compliance Certified by Bay Networks. They have successfully passed the Bay Networks Test Procedure, which tests conformance to the Bay Networks Year 2000 compliance definition. For more information, see the Bay Networks Year 2000 Web Site at *http://www.baynetworks.com/year2000/*.

Upgrading to Version 13.10

To upgrade BayRS to Version 13.10, or to upgrade Site Manager software to Version 7.10, see *Upgrading Routers to BayRS Version 13.xx*, in your upgrade package.

Upgrading ATM Configurations

If you are upgrading from a BayRS version earlier than 12.20 and you defined log event traps for ATM, ATM signaling, or ATM LAN emulation, you will need to redefine these traps.

The ATM, ATM signaling, and ATM LAN emulation log event messages changed in BayRS Version 12.20. The ATM_SIG entity (entity #95) no longer exists as a separate entity, but has been combined with the ATM entity (entity #78). Combining and reorganizing these entities resulted in changes to the ATM log event message numbers. New log events were added to the ATM_LE entity (entity #100), resulting in log event message number changes for LAN emulation as well.

You can view the new and modified ATM log event messages in the event database on the World Wide Web, or on the BayRS Online Library Version 13.10 CD. For information about how to access the event database, see “Event Database” on page 4.

Upgrading L2TP Configurations

If you have a BayRS Version 12.10 configuration file that includes L2TP operating on a router using BayRS Version 13.10, the router automatically upgrades the assigned user network addresses to an L2TP IP interface addresses. L2TP IP interface addresses are internal to the router. When communicating with the remote user, the router associates the user's IP address with an L2TP IP interface address that you configure.

The user network addresses assigned to Version 12.10 apply to the entire router. In Version 13.10, each slot has a unique L2TP IP address. Consequently, if the number of configured L2TP slots is greater than the number of configured assigned user network addresses, the router will not be able to upgrade every slot from a Version 12.10 configuration to a Version 13.10 configuration. For slots that exceed the number of assigned user network addresses, you will need to manually configure L2TP IP interface addresses. To do this, delete L2TP from the slot, then configure a new L2TP interface. Each slot must have L2TP IP interface addresses.

If the number of configured L2TP slots is less than or equal to the number of configured assigned user network addresses, the router automatically converts all assigned user network addresses to L2TP IP addresses.

Upgrading OSPF Configurations

When you upgrade BayRS from releases earlier than Version 12.20, there must not be an OSPF MTU interface mismatch. If a mismatch exists, adjacencies will not form between upgraded routers. All the OSPF routers forming adjacencies on a segment (broadcast, PPP, Point-to-Multipoint, or NBMA) should have the same OSPF MTU size. You can verify the OSPF MTU sizes from Site Manager or the Technician Interface.

BayRS Versions 12.20 and later comply with RFC 2178, which requires the OSPF MTU size feature.

Upgrading the BCC Help File

The following information updates instructions relating to the BCC Help file mentioned in *Upgrading Routers to BayRS Version 13.xx*.

If you received a flash card with the BayRS 13.10 (BCC 4.10) image, it should also contain the BCC Help file, *bcc.help*. The BCC looks for this file name as soon as you enter the first **help** <*option*> command after booting the router using the new Version 13.10 image.

If the *bcc.help* file is not already on the default volume in the router, you must transfer it from the BayRS Version 13.10 software CD to that volume. The BCC Help file on the BayRS software CD has the name *bcc_help*. When you transfer that file to the router, be sure to rename it as *bcc.help*. (The Version 13.10 router software is not configured by default to recognize the file name *bcc_help*.)

Event Database

With BayRS Version 13.10, you can view the event database on the World Wide Web and the BayRS Online Library Version 13.10 CD. To access the event database on the World Wide Web, go to:

http://support.baynetworks.com/library/tpubs/events

To access the event database on the BayRS Online Library Version 13.10 CD, follow the instructions in the CD booklet.

The event database includes a search facility that allows you to sort events by entity number, event number, severity, and text of the event message. For example, you can list only the warning messages for the IPX entity.

Quick2Config

Quick2Config® Version 1.3.2, which shipped with BayRS Version 12.20, was the final release of Quick2Config. Quick2Config Version 1.3.2 is not compatible with BayRS Version 13.10 or later, and there will be no new versions of Quick2Config for these releases. Bay Networks will maintain Quick2Config Version 1.3.2 until early 2001.

You can continue to configure routers with Site Manager and the BCC.

SunOS 4.1.4 Support for Site Manager

Customers using Site Manager with SunOS 4.1.4 must plan to migrate to a supported Solaris OS platform. Site Manager Version 7.20 will be the last release that will ship with SunOS support. Site Manager releases later than 7.20 will not work with SunOS, but will continue to work with Solaris and other supported operating systems.

Using the BCC

The Bay Command Console (BCC™) is a command-line interface for configuring Bay Networks devices. It also supports Technician Interface commands and scripts.

Before using the BCC, refer to the following sections listing the platforms, protocols, interfaces, and hardware modules that the BCC supports.

Platforms Supported

The BCC runs on AN®, ANH™, ARN™, ASN ®, System 5000™, and BN® platforms including ARE, FRE®, and FRE-2 processor modules. Each slot must have:

- 16 MB of dynamic RAM (DRAM)
- 2 MB of free memory available when you start the BCC

If you try to start the BCC with insufficient DRAM or free memory on a slot, the BCC returns an error message. In that case, use Site Manager instead of the BCC.

Number of BCC Sessions

You can open one BCC session per slot in read-write (configuration) mode. Other users can open additional BCC sessions in read-only (nonconfiguration) mode, depending on the memory resources available on the slot supporting your login session. When memory requirements are insufficient to support additional BCC sessions on a login slot, the system displays the following message:

`BCC requires 2MB of free memory. Current available memory is` *<current_available>* `bytes.`

All BCC sessions are mutually exclusive. If you make a change in a BCC session in read-write mode, this change does not appear in another BCC session.

BCC Help Initialization

Obtaining a response from a BCC help request may require an initialization time of about one minute. This initialization occurs only when issuing the first help command after booting the device. Subsequent requests for BCC help information take only one or two seconds.

Interfaces Supported

You can use BCC commands to configure the following physical/virtual interfaces:

- ATM
- Console
- DCM
- DSU/CSU
- Ethernet
- FDDI
- FE1
- FT1
- HSSI
- ISDN/BRI
- MCE1/MCT1
- Serial (synchronous)
- Token ring
- Virtual (referred to in Site Manager as Circuitless IP)

Tables 1 through 5 on pages 11 to 16 list the link and net modules that the BCC supports.

Global Protocols Supported

You can use BCC commands to configure the following global services:

- Access (multiuser access accounts)
- ARP
- BGP (including accept and announce policies)
- DNS
- DVMRP
- FTP
- HTTP
- IGMP
- IP (including access policies, static routes, and adjacent hosts)
- IPX (including static-netbios-route)
- IPXWAN
- NTP
- OSPF (including accept and announce policies)
- RIP (including accept and announce policies)
- SNMP
- Syslog
- Telnet
- TFTP

Interface Protocols Supported

You can use BCC commands to configure the following interface protocols:

- ARP
- ATM
- Dial backup
- Dial-on-demand
- DVMRP
- Frame relay (multiline not supported)
- IGMP
- IP
- IPX

- OSPF
- PPP (certain line parameters only; no multiline or multilink supported)
- Proprietary Standard Point-to-Point
- RIP
- Router Discovery (RDISC)

Getting Started

Caution: BCC configuration and **source** commands make immediate changes to the active device configuration. Read about the **source** command in *Using the Bay Command Console (BCC)*.

Before using the BCC, save your configuration files by copying them onto the same flash memory card using new file names.

To start the BCC, enter **bcc** at the Technician Interface prompt.

To display the online instructions for new BCC users, enter **help learning-bcc** at the bcc> prompt. To display a full summary of the Help features of the BCC interface, just enter the **help** command at any BCC prompt.

For more information about how to use the BCC interface, see *Using the Bay Command Console (BCC).*

For instructions on using the BCC to add and change configurable services, see the documentation for that service.

Deleting Interfaces with the BCC

Before using the BCC to delete an interface, make sure that you did not use Site Manager to configure the interface with a protocol that the BCC does not recognize. If you did, use Site Manager to delete the interface.

BCC show Command Documentation

The following table maps each BCC **show** command to the document that contains its description:

BCC show command	Where Documented
show access	*Using the Bay Command Console (BCC)*
show atm	*Configuring ATM and MPLS Services*
show bgp	*unavailable*
show bri	*Configuring Dial Services*
show classical-ip	*Configuring ATM and MPLS Services*
show config	*Using the Bay Command Console (BCC)*
show console	*Using the Bay Command Console (BCC)*
show dial	*Configuring Dial Services*
show dns	*Configuring IP Utilities*
show dsucsu	*Configuring WAN Line Services*
show dsx3	*Configuring ATM and MPLS Services*
show dvmrp	*unavailable*
show ethernet	*Configuring Ethernet, FDDI, and Token Ring Services*
show fddi	*Configuring Ethernet, FDDI, and Token Ring Services*
show frame-relay	*Configuring Frame Relay Services*
show ft1e1	*Configuring WAN Line Services*
show ftp	*Configuring IP Utilities*
show hardware	*Using the Bay Command Console (BCC)*
show hifn	*Configuring Data Compression Services*
show hssi	*Configuring WAN Line Services*
show http	*Managing Routers Using the HTTP Server*
show hwcomp	*Configuring Data Compression*
show igmp	*unavailable*
show interface	*Using the Bay Command Console (BCC)*
show ip	*unavailable*

(continued)

BCC show command	Where Documented
show ipx	*Configuring IPX Services*
show isdn-switch	*Configuring Dial Services*
show lane	*Configuring ATM and MPLS Services*
show mct1e1	*Configuring WAN Line Services*
show modem	*Configuring Dial Services*
show mtm	*unavailable*
show ntp	*Configuring IP Utilities*
show ospf	*unavailable*
show ppp	*Configuring PPP Services*
show process	*Using the Bay Comand Console (BCC)*
show rmon	*Configuring RMON and RMON2*
show serial	*Configuring WAN Line Services*
show snmp	*unavailable*
show sonet	*Configuring ATM and MPLS Services*
show syslog	*BayRS Version 13.10 Document Change Notice*
show system	*Using the Bay Command Console (BCC)*
show tcp	*Configuring IP Utilities*
show telnet	*Configuring IP Utilities*
show tftp	*Configuring IP Utilities*
show token-ring	*Configuring Ethernet, FDDI, and Token Ring Services*
show wcp	*Configuring Data Compression Services*

Identifying Board Types

Tables 1 through 5 identify the Board Type parameter values displayed by the BCC. Use the "Board Type" column to find, in alphabetical order, a hardware module in an AN, ANH, ARN, ASN, BN, or System 5000 router configuration.

Notes:

- You cannot use BCC commands to configure an X.25 PAD or V.34 console modem daughterboard for the ARN router. (Use Site Manager to configure these daughterboards.)
- Inserting a daughterboard into an AN base module redefines its module ID and board type.

Table 1 lists the AN and ANH board types.

Table 1. BCC Board Types: AN and ANH Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
andeds	1033	AN-ENET (2 Ethernet ports, 2 serial ports)
andedsg	1050	ANH-8 (2 Ethernet ports, 2 serial ports) and an 8-port Ethernet hub active for the first Ethernet port
andedsh	1035	ANH-12 (2 Ethernet ports, 2 serial ports) and a 12-port Ethernet hub
andedst	1034	AN-ENET (2 Ethernet ports, 2 serial ports, 1 token ring port)
andst	1037	AN-TOKEN (2 serial ports, 1 token ring port)
andstc	1091	AN-TOKEN with CSU/DSU (2 serial ports, 1 token ring port)
andsti	1038	AN-TOKEN with ISDN (2 serial ports, 1 token ring port)
ansdsedst	1041	AN-ENET/TOKEN (1 Ethernet port, 2 serial ports, 1 token ring port)
anseds	1024	AN-ENET (1 Ethernet port, 2 serial ports) with 16 MB DRAM
ansedsc	1090	AN-ENET with CSU/DSU (2 Ethernet ports, 2 serial ports)
ansedsf	1100	AN-ENET with T1/FT1 (2 Ethernet ports, 2 serial ports)
ansedsg	1047	ANH-8 (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgc	1094	ANH-8 with CSU/DSU (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub

(continued)

Table 1. BCC Board Types: AN and ANH Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Description
ansedsgf	1108	ANH-8 with T1/FT1 (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgi	1051	ANH-8 with ISDN (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsgj	1127	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and an 8-port Ethernet hub
ansedsgjx	1137	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and an 8-port Ethernet hub and DCM
ansedsgx	1048	ANH-8 with DCM (1 Ethernet port, 2 serial ports) and an 8-port Ethernet hub
ansedsh	1026	ANH-12 (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshc	1093	ANH-12 with CSU/DSU (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshf	1106	ANH-12 with T1/FT1 (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshi	1029	ANH-12 with ISDN (1 Ethernet port, 2 serial ports) and a 12-port Ethernet hub
ansedshj	1125	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and a 12-port Ethernet hub
ansedshjx	1136	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) and a 12-port Ethernet hub and DCM
ansedsi	1027	AN-ENET with ISDN (2 Ethernet ports, 2 serial ports) with 16 MB DRAM
ansedsj	1119	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) with 16 MB DRAM
ansedsjx	1133	AN-ENET (1 Ethernet port, 2 serial ports, 1 fractional E1 port) with 16 MB DRAM and DCM
ansedst	1025	AN-ENET/TOKEN (1 Ethernet port, 2 serial ports, 1 token ring port) with 16 MB DRAM
ansedstc	1092	AN-ENET/TOKEN with CSU/DSU (1 Ethernet port, 2 serial ports, 1 token ring port)

(continued)

Table 1. BCC Board Types: AN and ANH Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Description
ansedsti	1028	AN-ENET/TOKEN with ISDN (1 Ethernet port, 2 serial ports, 1 token ring port)
ansedstj	1123	AN-ENET (1 Ethernet port, 2 serial ports, 3 fractional E1 ports) with 16 MB DRAM
ansedstjx	1135	AN-ENET (1 Ethernet port, 2 serial ports, 3 fractional E1 ports) with 16 MB DRAM and DCM
ansedstx	1058	AN-ENET/TOKEN with DCM (1 Ethernet port, 2 serial ports, 1 token ring port) with 16 MB DRAM
ansedsx	1055	AN-ENET with DCM (2 Ethernet ports, 2 serial ports)
ansets	1030	AN-ENET (1 Ethernet port, 3 serial ports) with 16 MB DRAM
ansetsg	1049	ANH-8 (1 Ethernet port, 3 serial ports) and an 8-port Ethernet hub
ansetsh	1032	ANH-12 (1 Ethernet port, 3 serial ports) and a 12-port Ethernet hub
ansetst	1031	AN-ETS (1 Ethernet port, 3 serial ports, 1 token ring port)
antst	1039	AN-TOKEN (3 serial ports, 1 token ring port)

Table 2 lists the BLN and BCN board types.

Table 2. BCC Board Types: BLN and BCN Modules

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
atmcds3	5120	AG13110115	ATM DS-3
atmce3	5121	AG13110114	ATM E3
atmcoc3mm	4608	AG13110112	ATM STS-3/STM-1 MMF
atmcoc3sm	4609	AG13110113	ATM STS-3/STM-1 SMF
comp	4353	AG2104037	Octal Sync with 32-context compression daughterboard
comp128	4354	AG2104038	Octal Sync with 128-context compression daughterboard

(continued)

Table 2. BCC Board Types: BLN and BCN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
de100	4864	50038	100BASE-T Ethernet
dst416	40	5740	Dual Sync with token ring
dtok	176	5710	Dual token ring
enet3	132	5505	Dual Ethernet
esaf	236	5531	Dual Sync Dual Ethernet with 2-CAM filters
		5532	Dual Sync Dual Ethernet with 6-CAM filters
esafnf	232	5431	Dual Sync Dual Ethernet without hardware filters
mce1ii120	190	AG2111002	120-ohm Dual Port Multichannel E1 (MCE1-II) for ISDN PRI and Leased Line
mce1ii75	188	AG2111004	75-ohm Dual Port Multichannel E1 (MCE1-II) for 75-ohm Leased Line
mct1	168	5945	Dual Port MCT1
osync	4352	5008	Octal Sync
qef	164	5950	Quad Ethernet with hardware filters
qenf	162	5450	Quad Ethernet without hardware filters
qmct1db15	5377	AG2111007	Quad Port MCT1 DB15
qmct1ds0a	5378	AG2104052	Quad Port MCT1 DB15 with DS0A
qtok	256	50021	Quad token ring
shssi	225	5295	HSSI
smce1ii120	191	AG2111001	120-ohm Single Port Multichannel E1 (MCE1-II) for ISDN PRI and Leased Line
smce1ii75	189	AG2111003	75-ohm Single Port Multichannel E1 (MCE1-II) for 75-ohm Leased Line
smct1	169	5944	Single Port MCT1e
sse	118	5410	Single Sync with Ethernet
sync	80	5280	Quad Sync
wffddi1m	193	5943	Hybrid FDDI with single mode on connector B
wffddi1mf	197	5949	Hybrid FDDI with single mode on connector B and with hardware filters

(continued)

Table 2. BCC Board Types: BLN and BCN Modules *(continued)*

BCC Board Type	Technician Interface or MIB Module ID	Site Manager Model Number	Description
wffddi1s	195	5942	Hybrid FDDI with single mode on connector A
wffddi1sf	199	5948	Hybrid FDDI with single mode on connector A and with hardware filters
wffddi2m	192	5930	Multimode FDDI
wffddi2mf	196	5946	Multimode FDDI with hardware filters
wffddi2s	194	5940	Single Mode FDDI
wffddi2sf	198	5947	Single Mode FDDI with hardware filters

Table 3 lists the ASN board types. Table 4 lists the ARN board types.

Table 3. BCC Board Types: ASN Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
asnqbri	2560	Quad BRI Net Module
denm	1280	Dual Port Ethernet Net Module
dmct1nm	2944	Dual Port MCT1 Net Module
dsnm1n	1540	Dual Port Synchronous Net Module
dsnm1nisdn	1588	ISDN BRI/Dual Sync Net Module
dtnm	2048	Dual Port Token Ring Net Module
mce1nm	2816	MCE1 Net Module
mmasmbdas	1833	Hybrid PHY B FDDI Net Module
mmfsddas	1793	Multimode FDDI Net Module
qsyncm	1664	Quad Port Synchronous Net Module
se100nm	2304	100BASE-T Ethernet Net Module
shssinm	3584	HSSI Net Module
smammbdas	1825	Hybrid PHY A FDDI Net Module
smfsddas	1801	Single Mode FDDI Net Module
spex	512	SPEX Net Module
spexhsd	769	SPEX - Hot Swap Net Module

Table 4. BCC Board Types: ARN Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
arn7sync	8873	ARN Seven-port Serial Expansion Module
arndcsu	8768	ARN 56/64K DSU/CSU Adapter Module
arne7sync	8872	ARN Seven-Port Serial Expansion Module, with 1 Ethernet Port
arnentsync	8864	ARN Ethernet and Tri-Serial Expansion Module
arnfe1	8780	E1/FE1 DSU/CSU Adapter Module
arnft1	8776	T1/FT1 DSU/CSU Adapter Module
arnis	8784	ARN ISDN BRI S/T Adapter Module
arnisdnu	8800	ARN ISDN BRI U Adapter Module
arnisdnu	8880	ARN Token Ring and Tri-Serial Expansion Module
arnmbenx10	8896	ARN Ethernet Base Module - xxMB DRAM with DCM
arnmbsen	8720	ARN Ethernet Base Module with 0, 4, 8, 16, or 32 DRAM
arnmbstr	8704	ARN Token Ring Base Module with 0, 8, 16, or 32 MB DRAM
arnpbenx10	8928	ARN Ethernet Expansion Module with DCM
arnpbtenx10	8960	ARN Ethernet and Tri-Serial Expansion Module with DCM
arnsenet	8832	ARN Ethernet Port Expansion Module
arnssync	8736	ARN Serial Adapter Module
arnstkrg	8816	ARN Token Ring Expansion Module
arntsync	8848	ARN Tri-Serial Port Expansion Module

Table 5 lists the System 5000 board types.

Table 5. BCC Board Types: System 5000 Modules

BCC Board Type	Technician Interface or MIB Module ID	Description
asnqbri	2560	Router Quad Port ISDN BRI Net Module
atm5000bh	524544	Centillion Multiprotocol Engine
denm	1280	Router Dual Ethernet Net Module
dmct1nm	2944	Router Dual Port MCT1 Net Module
dsnm1n	1540	Router Dual Synchronous Net Module
dtnm	2048	Router Dual Token Ring Net Module
iqe	1408	5380 Ethernet Router Module
iqtok	2176	5580 Token Ring Router Module
mce1nm	2816	Router MCE1 Net Module
mmasmbdas	1833	Router Hybrid PHY B FDDI Net Module
mmfsddas	1793	Router Multimode FDDI Net Module
qsyncnm	1664	Router Quad Port Synchronous Net Module
se100nm	2304	Router 100BASE-T Ethernet Net Module
shssinm	3584	Router HSSI Net Module
smammbdas	1825	Router Hybrid PHY A FDDI Net Module
smfsddas	1801	Router Single Mode FDDI Net Module

Sending BCC Feedback

After you use the BCC, we welcome your feedback. Please visit the BCC Web site at the following URL, where you can leave us a message:

http://support.baynetworks.com/library/tpubs/bccfeedbk

New Features in BayRS Version 13.10

BayRS Version 13.10 provides the following new features.

BaySecure FireWall-1

BayRS 13.10 provides support for ISDN interfaces, as well as support for backup management stations.

Backup management stations provide the redundancy required to use BaySecure FireWall-1 in large enterprise networks. Using Site Manager, you can configure up to two backup management stations. Then if your router loses communication with its firewall management station, a backup firewall management station automatically establishes communication with the router so that the firewall security remains intact and the logging of firewall statistics continues.

BaySecure FireWall-1 does not require that a backup management station remain dormant until called into service when a another firewall management station fails. A backup management station can simultaneously be a working firewall management station for another firewall.

Backup Management Station Selection

A router connects to a backup firewall management station upon termination of the TCP connection (with TCP_ABORT) between the current firewall management station and the router.

Note: When an event, like the failure of a LAN, prevents communication between the router and the firewall management station, the firewall management station closes the TCP connection from its end when data does not flow from the idle TCP connection. However, the router does not close the TCP connection from its end for a period of time determined by the TCP keepalive timer. The TCP keepalive timer in the firewall application on the router periodically checks the TCP connection before the router aborts the idle TCP connection.

When a firewall management station becomes disconnected from the router, the router begins a round-robin selection process where it continuously tries to connect to another management station at 40-second intervals. The order of the round-robin selection is primary, first backup, and then second backup management station.

For example, if the connection between the router and the primary management station fails, the router tries to connect to the first backup management station. If the router connects to the first backup management station and that connection later fails, the router tries to connect to the second backup management station before it tries to connect to the primary management station again.

BCC show config Options

The BCC **show config** command has new options and output behavior, starting with the 13.10 Release of BayRS, as follows:

show config	Show the configuration of the current object only. Example: **show config**
show config <*BCC_instance_ID*>	Show the configuration of the specified object. Example: **show config ip/1.2.3.4/255.0.0.0**
Command Options (combine to customize **show config** output):	
-compact	Show the configuration without navigation (**back**) commands. Example: **show config -compact**
-recursive	Show any dependent objects configured on this object. Examples: **show config -recursive** **show config -compact -recursive** **show config ip/1.2.3.4/255.0.0.0 -recursive**
-verbose	Show the configuration, including all configurable parameters, including those set to a default value. Examples: **show config -verbose** **show config -recursive -verbose** **show config ip/1.2.3.4/255.0.0.0 -recursive -verbose**
-all	Show the total device configuration. Examples: **show config -all** **show config -all -verbose**
-file <*filename*>	Save the output of this command to a file. Examples: **show config -all -file boston.config** **show config -all -recursive -verbose -file boston.config** **show config ip/1.2.3.4/255.0.0.0 -file boston.config**

BCC Support for Dial-on-Demand Service

You can now use the BCC to configure dial-on-demand service on your router. For information, see *Configuring Dial Services*.

BGP Configuration

The following features are new for BGP in BayRS Version 13.10. For more information about BGP, see Chapter 8 of *Configuring IP Services.*

Route Flap Dampening

The frequent change of network reachability information that can be caused by an unstable route is commonly referred to as *route flap*. Route flap *dampening* is a technique for suppressing information about unstable routes. BayRS Version 13.10 supports dampening of unstable EBGP routes.

To monitor BGP for route flaps, you set the route dampening parameter on a BGP accept policy that matches the route. BGP creates a penalty value for the route and sets the value to 0. BGP increments the penalty each time the route flaps.

BGP provides a *route flap dampening template* that allows you to control the way BGP evaluates a route's penalty and how, based on the penalty, it decides to suppress or unsuppress the route.

For information about BGP route flap dampening, see Chapter 8 of *Configuring IP Services.*

Configuring EBGP for Route and Traffic-Load Balancing

EBGP route balancing and traffic-load balancing are two techniques that allow an EBGP speaker to distribute routes to the same destination among multiple equal-cost paths.

In both techniques, EBGP uses equal cost multipath (ECMP) routes submitted statically to the IP routing table. You can configure an EBGP speaker to use ECMP static routes in the IP routing table for route balancing and traffic-load balancing.

For information about configuring EBGP for route balancing and traffic-load balancing, see Chapter 8 of *Configuring IP Services.*

Data Compression Enhancements

BayRS 13.10 adds BCC commands for changing the compression mode, disabling and reenabling WCP, and adding WCP software compression for PPP and frame relay services in several different contexts. It also adds descriptions of the **show** commands for both hardware and software data compression.

DHCP Server

DHCP now implements a DHCP server feature that complies with RFC 2131. The DHCP server manages client IP addresses and interacts with the NetID Server Manager to configure and maintain client address ranges and configuration options.

For the DHCP server to operate, you must first install the NetID Server Manager on a UNIX or NT workstation and configure it to communicate with the DHCP server. Typically, you install the NetID Server Manager on the same workstation as the one that contains the NetID database.

For information about DHCP server, see *Configuring SNMP, BootP, DHCP, and RARP Services*.

DLSw PU Type 4 Device Support

DLSw now supports PU type 4 devices. A PU (physical unit) is a component of the network that manages and monitors the resources (such as attached links and adjacent link stations) associated with the node. PU type 4 devices are subarea nodes that use network addresses for routing and maintain routing tables that reflect the configuration of the network.

PU type 4 devices include IBM 3720, 3725, and 3745 front end processors (FEPs). These FEPs provide enhanced SNA services not provided by routers. The router allows connection of the FEPs using SDLC or LLC. LAN-to-LAN, SDLC-to-SDLC, LAN-to-SDLC, and SDLC-to-LAN connections are supported.

The FEPs communicate using FID4 data flows. FID4 is the SNA protocol format used between two adjacent subarea nodes. This protocol format is supported by single-switch and dual-switch operation of DLSw. For information about DLSw, see *Configuring DLSw Services.*

Domain Name Server (DNS) Proxy

The DNS proxy server is a system solution that lets the router act as a DNS server. DNS clients can configure an interface on the router as their DNS server. The DNS proxy server on the router has a list of servers to contact on behalf of the client.

Using the DNS proxy server feature, a network administrator can statically configure hosts to use the IP address of the DNS proxy server on the router. If DNS servers change or physically move, the administrator has to change the list of DNS servers only on the router, rather than on each individual client. For information about the DNS Proxy Server, see *Configuring IP Utilities*.

Generic Routing Encapsulation

Generic Routing Encapsulation (GRE), which is defined in RFCs 1701 and 1702, is a generalized protocol that defines a method for encapsulating any payload inside any network (layer 3) protocol. For BayRS Version 13.10, GRE allows the layer 3 protocol IPX, as well as IP, to be encapsulated in IP. GRE tunnels are manually configured on the routers. For information about GRE, see Chapter 13 of *Configuring IP Services*.

HTTP Server

For Version 13.10, the HTTP Server contains many enhancements that improve performance, but that are not otherwise visible to the user. Two key elements that affect what the user sees are improved security and the ability to access the monitored router using its domain name instead of its IP address.

Improved Security

While continuing to support basic access authentication using a user name and password, Version 13.10 also implements (RFC2069-compliant) digest authentication, based on a challenge-response model. Most browsers, however, do not yet support digest authentication. Although you can configure digest authentication for Bay Networks routers, leave this parameter at the default setting of basic authentication.

Domain Name Access

By setting the Domain Name parameter, you can access the server by a domain name, rather than by IP address. Set the Domain Name parameter to the domain name that a DNS lookup would return for the router. The name can consist of any valid string of characters that constitute a domain name.

HTTP Server Parameters

The HTTP Server has removed two obsolete configuration parameters, cache-aging-timer and max-cached-archives, and added two new parameters, authentication and domain name. Uses of the new parameters are described in *Managing Routers Using the HTTP Server.*

IP Multicasting Configuration

The following features are new for DVMRP and IGMP Relay in BayRS Version 13.10. For more information about DVMRP and IGMP Relay, see *Configuring IP Multicasting and Multimedia Services.*

DVMRP BCC Support

You can now use the BCC to configure DVMRP globally and on an IP interface, and to configure DVMRP tunnels. For information about configuring DVMRP using the BCC, see Chapter 4 of *Configuring IP Multicasting and Multimedia Services.*

DVMRP Policies

BayRS Version 13.10 supports DVMRP accept unicast route policies and accept policies, as well as both the announce and the ignore functions for DVMRP announce policies (earlier versions of BayRS supported only the ignore function for DVMRP announce policies).

- An accept unicast route policy causes DVMRP to copy the routes you specify from the IP unicast routing table and inject them into the DVMRP routing table. You must configure an inject unicast route policy if you are connecting a multicast router running DVMRP to an IGMP Relay device.
- An accept policy causes DVMRP to filter incoming advertisements.
- An announce policy governs the propagation of DVMRP routing information.

For information about configuring DVMRP policies, see Chapter 4 of *Configuring IP Multicasting and Multimedia Services.*

IGMP Relay

An IGMP Relay device is a unicast router with an interface to a multicast router and interfaces to one or more networks containing network hosts. For BayRS Version 13.10, the multicast router can run DVMRP, as well as MOSPF.

A router configured as an IGMP Relay device provides the following group registration services for an IP multicast router:

- Solicits multicast group membership information by sending IGMP host membership queries to hosts on its attached local networks
- Receives host membership reports and unsolicited join messages from hosts on attached networks and forwards them to the attached multicast router
- Forwards multicast data to group members on locally attached networks

For information about IGMP Relay, see Chapter 9 of *Configuring IP Multicasting and Multimedia Services.*

IP Security (IPsec)

The Internet poses the challenge of providing a secure means of communicating that is both scalable and interoperable with different security schemes. IP Security (IPsec) is a set of protocols being developed by the IETF to provide secure communication over IP networks. These standards are designed to ensure secure, private communication for remote access, extranet, and intranet virtual private networks (VPNs). IPsec is designed to work flexibly with different encryption algorithms, authentication methods, and key exchange methods.

The Bay Networks implementation of IPsec supports the Encapsulating Security Payload (ESP) protocol, which uses the Data Encryption Standard (DES) to encrypt the packet payload, and Message Digest 5 (MD5) to provide authentication. Because ESP allows the user to implement null encryption, ESP provides the same capabilities as the Authentication Header (AH) protocol. For this reason, Bay Networks supports only ESP, not AH.

For BayRS Version 13.10, key management is manual.

IPsec supports tunnel mode and transport mode; the Bay Networks implementation of IPsec supports only tunnel mode.

For BayRS Version 13.10, the Bay Networks implementation of IPsec provides network layer (layer 3) security services for WAN communications on AN, ARN, ASN, and System 5000 routers. For more information about IPsec and instructions on how to configure it on a router, see *Configuring IP Security Services*.

L2TP Support (RFC 1877)

Bay Networks has implemented RFC 1877, "IP Control Protocol (IPCP) Name Server Addresses," for Layer 2 Tunneling Protocol (L2TP) connections. This name server address (NSA) feature enables remote hosts dialing in to a Bay Networks router acting as an L2TP network server (LNS) to obtain NSAs from either the LNS or a RADIUS server.

To use the NSA feature, users at remote sites configuring their dial-up connections in Windows® 95, Windows 98, or Windows NT®, must specify that their connections will use Server assigned name server addresses to indicate that a remote server provides NSAs.

If a user does not select the Server assigned name server addresses setting, the connection uses the NSAs that the user enters in the TCP/IP Settings window. The NSA feature is disabled for the connection.

When users specify that they want to use server-assigned NSAs, they should not enter primary and secondary domain name server (DNS) and WINS name server addresses (also called *NetBIOS name server addresses* or *NBNS addresses*).

Instead, when a user dials in, the LNS or RADIUS server automatically assigns name server addresses for the connection. If a name server address changes, the network administrator can change it once at the LNS or RADIUS server site; every remote user is not required to enter a new address. For information about L2TP, see the *BayRS Version 13.10 Document Change Notice*.

Multiuser Access Control

Previous versions of the BCC included two user logins:

- Manager login that allowed you to enter any system-level command and allowed read-write access to the device configuration
- User login that allowed you to enter only user-level system commands and allowed read-only access to the device configuration

Multiuser access allows you to configure multiple user logins (each with a distinct user name, password, and privilege levels) to access the router simultaneously. For information about multiuser access control, see *Using the Bay Command Console (BCC)*.

Multiprotocol Label Switching (MPLS)

MPLS is an emerging Internet Engineering Task Force (IETF) standard that is currently in draft form. Its primary goal is to integrate label-swapping and forwarding with network layer routing.

Using MPLS, a router assigns a label that defines a specific packet stream. The router then forwards packets based on these fixed-length labels. The labels are associated with inbound and outbound interfaces. Assigning labels to packets or packet streams increases the transmission speed of your network.

Protocol Statistics for MPLS

The HTTP Server interface for 13.10 contains an additional folder icon for displaying MPLS statistics. The following information summarizes these statistics and how to get them using the HTTP Server interface.

Clicking on Statistics > Protocols > MPLS in the navigational frame reveals the following subordinate links: MLM Interfaces, MLM Sessions, MLM Connections, LDP Sessions, and LDP Information. Click on each link to display the statistics for its associated entity. For information, see *Managing Routers Using the HTTP Server.*

To see these statistics	Use this path
MPLS Label Manager (MLM) interfaces	Statistics > Protocols > MPLS > MLM Interfaces
MPLS Label Manager sessions	Statistics > Protocols > MPLS > MLM Sessions
MPLS Label Manager virtual circuits	Statistics > Protocols > MPLS > MLM Connections
Label Distribution Protocol (LDP) sessions	Statistics > Protocols > MPLS > LDP Sessions
Label Distribution Protocol label information base	Statistics > Protocols > MPLS > LDP Information

MPLS Routing Support

The BayRS 13.10 version of MPLS, which operates only on the ARE for the BN router, has been qualified with the Ericsson implementation of MPLS. The Ericsson implementation supports RIP version 2 and static routes. For information about MPLS, see *Configuring ATM and MPLS Services*.

MPOA Enhancements

Bay Networks has supported MPOA Server since BayRS Version 12.20. BayRS Version 13.10 contains the following enhancements:

- IP route table monitoring with MPOA purges used for updates
- NHRP support over LANE

For information about MPOA, see *Configuring ATM and MPLS Services*.

PVC Operations and Management

The PVC Operations and Management (OAM) feature provides a mechanism by which ATM devices can receive prompt failure information. Traditionally, the remote ATM device receives failure information from a non-ATM source such as a routing protocol that operates above the ATM layer. This type of notification can take a significant amount of time. The PVC OAM feature updates the remote device over the ATM layer, decreasing the failure notification to only a few seconds. For information about OAM, see *Configuring ATM and MPLS Services*.

Syslog Support

You can now use the BCC to configure Syslog services on your router. For information, see the *BayRS Version 13.10 Document Change Notice*.

Virtual Router Redundancy Protocol (VRRP)

VRRP enables you to configure router redundancy, using virtual routers, to protect a network from the irrecoverable failure of an entire router. VRRP manages a virtual router, which is a software-defined object that corresponds to an IP address on a LAN segment. A virtual router typically exists on multiple routers running VRRP. One of the VRRP routers acts as the master virtual router for an IP address, while VRRP routers act as backup virtual routers. BayRS 13.10 supports VRRP over LANE.

For information about VRRP, see *Configuring VRRP Services*.

WEP over Dial Services

You can now configure the WAN Encryption Protocol (WEP) for dial-on-demand, dial backup, and bandwidth-on-demand circuits for the AN, ARN, ASN, BN, and System 5000 routers.

If you configure WEP to work with dial backup service, encrypted data travels over the backup circuit if the primary line fails. In addition, the maximum NTP timer value has been expanded so that routers using WEP and dial services can now use NTP to synchronize time for WEP security purposes, without the overhead of excessive dial connections.

New Hardware for BayRS 13.10

BayRS Version 13.10 supports the following new hardware.

ARN E7S Support

BayRS supports the following new expansion modules for the ARN router:

- E7S (one Ethernet port plus seven serial ports)
- 7S (seven serial ports -- RS232, V35, RS422, X.21)

You cannot use NetBoot on ports 6, 7, 8, and 9.

BCC Support for the FRE2-060E Processor Module with Advanced Compression Coprocessor

BayRS 13.10 provides BCC support for the FRE2-060E processor module with advanced hardware compression capabilities that resides in the BN router.

BCC Support for the FRE-2-060E Processor Module

BayRS 13.10 provides BCC support for the FRE2-060E processor module that resides in the BN router.

Support for 64 MB ATM Routing Engine

BayRS 13.10 supports 64 MB ATM Routing Engine ILIs. The new AREs offer 64 MB of SRAM and 6 MB of DRAM, which allow for greater scalability and performance.

Table 6. 64 MB ATM Routing Engine Specifications

Part Number	Description
AG1304020	64M/6M ARE with OC3 MMF ILI
AG1304015	64M/6M ARE with OC3 SMF ILI
AG1304016	64M/6M ARE with DS-3 ILI
AG1303021	64M/6M ARE with E3 ILI

Guidelines for Working with BayRS Version 13.10

Note the following guidelines when using BayRS Version 13.10. These guidelines supplement the instructions in the Version 13.10 documentation set.

Amendment to Configuring PPP Services

You can now configure the following PPP line features using the BCC:

- Convergence timer
- Asynchronous modem control character map
- Maximum receive unit (MRU)
- RFC 1661 (MRU) compliance
- Authentication protocols

These features are relevant only for PPP dial connections. To customize these connections using the BCC, you must access the PPP dial interface or dial circuit object.

For instructions on how to customize these features, see *Configuring Dial Services*. Specifically, to customize all features except the authentication protocols, see Chapter 9, "Modifying PPP Dial Interfaces in a Pool." To customize the authentication protocols CHAP and PAP, see Chapter 12, "Modifying PPP Authentication Information."

AN/ANH and ARN Guidelines

Note the following operational guidelines when using AN, ANH, or ARN routers.

Allocating Memory on ARN Routers

Although you can change the default memory allocation on other Bay Networks router platforms, the ARN platform does not support this "buffer carving" feature.

On the ARN, Site Manager does not support the Admin > Kernel Configuration option, and the Technician Interface does not support the **set** command for wfKernCfgParamEntry objects. Attempting to set wfKernCfgParamGlobMem on the ARN results in a warning message.

DSU/CSU Test LED Remains On After Reset

The ARN DSU/CSU Test LED properly goes on when the interface enters test or loopback mode. However, the LED remains on after resetting the DSU/CSU module, even though all looping terminates and the module hardware resets.

Restarting the router turns the LED off. However, this action is not necessary for proper operation of the DSU/CSU interface.

Network Booting on DSU/CSU Interfaces

AN and ANH DSU/CSU interfaces do not support network booting in BayRS Version 13.10. The ARN DSU/CSU supports network booting only over interfaces configured for 64 Kb/s Clear Channel service.

ARN Router Not a Supported DVS RADIUS Client

The ARN router is not a supported DVS RADIUS client.

BayRS Version 13.10 Flash Memory Requirements

BayRS Version 13.10 software ships on the following flash memory cards:

Platform	Flash Memory Required	Associated Software Suites
AN/ANH	8 or 16 MB	corp_suite, ip_access, office_suite
ARN	8 or 16 MB	corp_suite, ip_access, office_suite
ASN	8 or 16 MB	corp_suite, lan_suite, system_suite, wan_suite
BN	8 or 16 MB	atm_suite, corp_suite, lan_suite, system_suite, vnr_suite, wan_suite
System 5000	8 or 16 MB	corp_suite, lan_suite, system_suite, vnr_suite, wan_suite

Configuring PU 4 and SDLC Link Stations

If you use PU 4 devices with SDLC and modulo 128, set the SDLC parameters MAXOUT and MAXIN to 127. You see these parameters in the SDLC Link Station Configuration window. For instructions on setting these parameters, see *Configuring SDLC Services*.

Creating Multiple GRE Tunnels

When creating multiple GRE tunnels dynamically, you can configure a maximum of five point-to-point GRE tunnels. In multipoint configurations, you can configure 64 GRE tunnels per interface.

FireWall-1 Redundant Management Scripts

Note: The information contained in this section supersedes the information contained in the section "Transferring Security Policy and Configuration Files" found in Chapter 2 of *Configuring BaySecure FireWall-1*.

Firewall backup management stations must have the same security policies and configuration files that the primary firewall management station uses. Bay Networks has provided script files to make it easy to synchronize firewall management stations. The script files enable you to use a single command, **fwfilex**, to easily package files associated with a management station's security environment. You then manually transfer the files to other firewall management stations.

You can get these script files from the customer service Web page at *http://support.baynetworks.com/software*. Under Bay Networks Routers, select Router Software and click on Go. The firewall scripts are located under BayRS in Firewall Scripts.

Note: The redundant management scripts do not currently support cross-platform redundancy. You can use these scripts only when transferring from one Windows NT platform to another, or from one UNIX platform to another.

Preparing and Transferring Firewall Files Between Windows NT Platforms

When you complete the following steps, the Windows NT platforms are synchronized and ready to be used in a redundant firewall management configuration:

1. **Ensure that the files *zip.exe, unzip.exe,* and *fwfilex.cmd* reside in the FireWall-1 bin directory (typically *\WINNT\FW1\bin*).**
2. **Enter the command fwfilex -i** *<filename>* **to package the firewall environment (that is, firewall policies, logs, objects, and so on) into a single file.**
3. **Using FTP, copy, or another transfer utility, manually transfer the file <*filename*> from one Windows NT machine to another.**
4. **On the destination machine, use the command fwfilex -o** *<filename>* **to unpackage the firewall environment.**

IP Fragmentation Not Supported over GRE Tunnels

IP packets will not be fragmented when encapsulated at the tunnel ingress point. If necessary, you can set MTU sizes to values large enough to prevent fragmentation on relevant interfaces on the GRE tunnel ingress router. Alternatively, you can configure your system to send MTU sizes less than the MTU sizes of the relevant interfaces on the GRE tunnel ingress router.

IP Security (IPsec) Executable

To use the DES-56 IPsec Option to perform IPsec ESP tunnel mode encryption and authentication, you must purchase a separate CD containing the cryptographic API executable (*capi.exe*) for BayRS 13.10 software. Purchase this CD for the router platform on which you plan to install the IPsec software.

Adding the IPsec File to the BayRS 13.10 Base Kernel

To use IPsec, you must use Image Builder to add an IPSec file to the BayRS 13.10 base kernel. The IPSec file is located on a separate CD, which ships with the IPsec feature. To install IPsec, follow the instructions included on the IPsec CD.

To use IPsec, you do not need to modify or add anything to Site Manager 7.10.

Multiuser Access

To use the multiuser access feature, see *Using the Bay Command Console (BCC)* and the following guidelines.

Sharing BCC Multiuser Access Profiles

To share user access profiles configured on one router across multiple routers:

1. **Navigate in BCC configuration mode to a multiuser access context that you want to replicate on another router.**
2. **From the desired context, enter the following command:**

   show config -recursive -file *<filename>*
3. **Transfer the file from the local router to a target router.**
4. **Log on to the target router and enter BCC configuration mode.**
5. **Use the BCC source command to import access profiles from the transferred file into the device active configuration.**
6. **Exit, then reenter the BCC on the target router.**
7. **Enter show config -all to see your changes.**

For more information about using the **show config** and **source** commands, see *Using the Bay Command Console (BCC)*.

BCC Lock Messages

Multiuser access includes messages that identify which user has exclusive read-write access to the device configuration.

The additional lock messages take the generic form:

`read-write mode in use by` *<login-id>* `from` {*console* | *<ip address>*}`, use -force to override.`

Example:

```
read-write mode in use by testuser1 from 192.168.133.99, use -force
to override
```

This message appears when a user in BCC config mode is logged in using a telnet session. The message contains the user's login name and the IP address of the workstation from which the user initiated the session.

Example:

```
read-write mode in use by Manager from console, use -force to
override
```

This message appears when the user in BCC config mode is logged in at the console connected to the router.

Example:

```
SNMP user from 192.168.133.99 has the configuration locked, use
-force to override.
```

This message appears when an SNMP station has locked, exclusive read-write access to the device configuration. The message identifies "SNMP" and the IP address of the workstation from which that user initiated the session.

For information on SNMP locking, see *Configuring SNMP, BootP, DHCP, and RARP Services.*

Example:

```
SNMP General Set Error. Machine is currently locked by manager
255.255.255.255
```

This message appears when a Site Manager user attempts to open a dynamic configuration session on the same box with a BCC user currently in configuration mode.

The user login and the string 255.255.255.255 indicate to the Site Manager user that this is a BCC session.

Example:

```
Snmp Error: Setting File System Action.
```

This message appears when a Site Manager user attempts to use File Manager to transfer a file to or from a router that has a BCC user in configuration mode.

Password Command

As a result of the new multiuser access feature, the syntax for the **password** command has been modified, as follows:

password [**Manager** | **User** | *<username>*]

username is the login name for a specific user.

For the **password** *<username>* command to work, the system manager must first use the BCC interface to define (configure) user groups and names. See Appendix A of *Using the Bay Command Console (BCC)* for information about how to complete this task.

System prompts displayed by the **password** command remain unchanged.

Note that the system software immediately encrypts any new password you enter for <*username*> and stores it in encrypted form only.

NAT Anomalies

NAT exhibits the following anomalies in BayRS 13.10.

Configuring NAT Dynamically

When you configure a local or global interface for NAT in dynamic mode, the router returns an SNMP set error. However, this error does not affect the configuration of the router.

Deleting NAT from a Router

If you delete NAT from a router, all previously configured instances of static entries will remain in the router MIB. You can delete the instances using the Technician Interface.

Outbound LAN Traffic Filters

When implementing outbound traffic filters for LAN protocols, note that in some configurations the filters may cause a decline in throughput performance. For LAN circuits where the forwarding rate of the router is critical, you should monitor the throughput performance after configuring outbound traffic filters. If you notice an unacceptable performance degradation, try using inbound traffic filters.

Protocol Prioritization No Call Filters and TCP Applications

Using a no call filter that applies to any TCP application can cause TCP to retransmit the filtered packet.

When two routers running a TCP application are connected using a demand line, and the demand line becomes inactive, the TCP application remains inactive.

If a demand line configured with a no call filter goes down, the no call filter drops any TCP packets it receives. Because TCP never receives an acknowledgment for transmitting its packets, the TCP application continues to retransmit packets until the connection eventually times out and the application stops operating.

Note: No call filters are specific to dial services. For additional information about traffic filters and protocol prioritization, see *Configuring Traffic Filters and Protocol Prioritization.*

Support for Strata-Flash Card

BayRS Version 13.10 supports the Strata-Flash card on AN, ANH, ARN, ASN, and BN routers. For full details about flash cards that BayRS 13.10 supports, see “Flash Memory Cards Supported” on page 48.

WEP Executable

To use the DES-40 WAN Encryption Option or DES-56 WAN Encryption Option to perform PPP or FR layer 2 encryption, you must purchase a separate CD containing the WEP executable (*wep.exe*) for BayRS 13.10 software.

To install WEP on a router, you must first add the WEP executable to your BayRS 13.10 base kernel using Image Builder in Site Manager.

You can purchase two WEP executables based on the key size: a 40-bit version and a 56-bit version, which are included on separate CDs.

You must purchase three CDs when ordering the WEP protocol for BayRS software:

- Base BayRS 13.10 CD, which contains no WEP functions
- 40-bit WEP CD, which contains the 40-bit executable file
- 56-bit WEP CD, which contains the 56 bit executable file

To configure WEP, you do not need to modify Site Manager.

X.25 PVCs

BayRS Version 13.10 software supports X.25 PVCs for X.25 IPEX Gateway services only.

Operating Limitations

Be aware of the following limitations when using BayRS 13.10.

Restriction When Deleting ATM from a Router if Signaling Is Enabled

Do not delete ATM from a router if you enabled signaling on an ATM circuit. Otherwise, Site Manager, the BCC, or the Technician Interface will restart after a few minutes.

Restriction if Signal Ports Settings on a Switch and Router Conflict

If you are using a switch with signal ports set to V3.1, be sure to set the signaling setting on the router to V3.1. If you accept the default setting of V3.0 for the router, the router will fault repeatedly until you change the setting to V3.1.

Restriction When Creating FTP from the BCC

From the BCC, if you create FTP on the router, then delete it and recreate it, the BCC will fault. In this case, you must restart the BCC and create FTP on the router again.

Restriction When Deleting a Hybrid Mode Permanent Virtual Circuit (PVC)

If you configure SRB on a router, do not delete hybrid mode PVCs. Otherwise, all slots will restart.

Restriction When Using DLSw/APPN Boundary Port with AS400s and Other Adjacent Link Stations

Do not configure any explicit APPN adjacent link stations on the DLSw/APPN boundary (VCCT) port, unless you are certain that the adjacent link station (for example, an AS400) will not attempt to connect to the APPN node. Otherwise, the DLSw/APPN boundary (VCCT) function will fail to operate correctly and the router may restart.

Restriction When Virtual Channel Connections (VCCs) Become Inactive

On the ARE and 5782 MPE, BayRS 13.10 does not release virtual channel connections when they time out. To maintain the availability of VCCs for new activities, configure a LAN emulation client (LEC) other than the router to release the inactive VCCs.

Protocols Supported

BayRS Version 13.10 supports the following bridging/routing protocols and router configuration features:

- Advanced Peer-to-Peer Networking (APPN)
- AppleTalk and AppleTalk Update Routing Protocol (AURP)
- Asynchronous transfer mode (ATM)
- ATM Data Exchange Interface (ATM DXI)
- ATM Half Bridge (AHB)
- ATM LAN Emulation (802.3 and 802.5)
- Bandwidth Allocation Protocol (BAP)
- Binary Synchronous Communication Type 3 (BSC3)

- Bisync over TCP (BOT)
- Bootstrap Protocol (BootP)
- Border Gateway Protocol (BGP-3 and BGP-4)
- Classless interdomain routing (CIDR)
- Data compression (WCP and Hi/fn)
- Data link switching (DLSw)
- DECnet Phase IV
- Distance Vector Multicast Routing Protocol (DVMRP)
- Dynamic Host Configuration Protocol (DHCP)
- Encryption (WEP; proprietary)
- Exterior Gateway Protocol-2 (EGP-2)
- File Transfer Protocol (FTP)
- Frame relay (PVC, SVC)
- HP Probe
- Hypertext Transfer Protocol (HTTP)
- Integrated Services Digital Network (ISDN)
- Interface redundancy (proprietary)
- Internet Control Message Protocol (ICMP)
- Internet Gateway Management Protocol (IGMP)
- Internet Packet Exchange (IPX)
- Internet Protocol (IP)
- Internet Protocol Version 6 (IPv6)
- IPsec Encapsulating Security Payload (ESP)
- IPv6 PPP Control Protocol (IPv6CP)
- Internet Stream Protocol (ST2)
- Layer 2 Tunneling Protocol (L2TP)
- Learning Bridge
- Logical Link Control 2 (LLC2)

- Multi-Protocol over ATM (MPOA)
- Multicast OSPF (MOSPF)
- Multiprotocol Label Switching (MPLS)
- Native Mode LAN (NML)
- Network Time Protocol (NTP)
- Open Shortest Path First (OSPF)
- Open Systems Interconnection (OSI)
- Point-to-Point Protocol (PPP)
- Polled Asynch (PAS), also called Asynch Passthru over TCP
- Protocol prioritization
- Qualified Logical Link Control (QLLC)
- RaiseDTR dialup
- Remote Authentication Dial-In User Service (RADIUS)
- Resource Reservation Protocol (RSVP)
- Router discovery (RDISC)
- Router redundancy (proprietary)
- Routing Information Protocol (RIP)
- Service Advertisement Protocol (SAP)
- Simple Network Management Protocol (SNMP)
- Source Routing Bridge (SRB)
- Source Routing Bridge over ATM permanent virtual circuits (PVCs)
- Spanning Tree
- Switched Multimegabit Data Service (SMDS)
- Synchronous Data Link Control (SDLC)
- Telnet (inbound and outbound)
- Transmission Control Protocol (TCP)
- Transparent Bridge
- Transparent-to-Source Routing Translation Bridge

- Trivial File Transfer Protocol (TFTP)
- User Datagram Protocol (UDP)
- V.25bis dialup
- Virtual Network Systems (VINES)
- Virtual Router Redundancy Protocol (VRRP)
- X.25 with QLLC
- Xerox Network System (XNS)
- XMODEM and YMODEM

Standards Supported

Table 7 lists the Request For Comments (RFCs) and other standards documents with which Version 13.10 complies. BayRS Version 13.10 may support additional standards that are not listed in this table.

Table 7. Standards Supported by Version 13.10

Standard	Description
ANSI T1.107b-1991	Digital Hierarchy - Supplement to formats specifications
ANSI T1.404	DS3 Metallic Interface Specification
ANSI X3t9.5	Fiber Distributed Data Interface (FDDI)
Bellcore FR-440	Transport Systems Generic Requirements (TSGR)
Bellcore TR-TSY-000009	Asynchronous Digital Multiplexes, Requirements and Objectives
Bellcore TR-TSY-000010	Synchronous DS3 Add-Drop Multiplex (ADM 3/X) Requirements and Objectives
FIPS 46-2	Data Encryption Standard (DES)
FIPS 81	DES Modes of Operation (ECB, CBC)
IEEE 802.1	Logical Link Control (LLC)
IEEE 802.1Q	IEEE 802.1Q VLAN tagging
IEEE 802.3	Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
IEEE 802.5	Token Ring Access Method and Physical Layer Specifications

(continued)

Table 7. Standards Supported by Version 13.10 *(continued)*

Standard	Description
IEEE 802.1D	Spanning Tree Bridges
ITU Q.921	ISDN Layer 2 Specification
ITU Q.931	ISDN Layer 3 Specification
ITU X.25	Interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuits
RFC 768	User Datagram Protocol (UDP)
RFC 791	Internet Protocol (IP)
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 813	Window and Acknowledgment Strategy in TCP
RFC 826	Ethernet Address Resolution Protocol
RFC 827	Exterior Gateway Protocol (EGP)
RFC 854	Telnet Protocol Specification
RFC 855	Telnet Option Specification
RFC 856	Telnet Binary Transmission
RFC 857	Telnet Echo Option
RFC 858	Telnet Suppress Go Ahead Option
RFC 859	Telnet Status Option
RFC 860	Telnet Timing Mark Option
RFC 861	Telnet Extended Options: List Option
RFC 863	Discard Protocol
RFC 877	Transmission of IP Datagrams over Public Data Networks
RFC 879	TCP Maximum Segment Size and Related Topics
RFC 888	"STUB" Exterior Gateway Protocol
RFC 894	Transmission of IP Datagrams over Ethernet Networks
RFC 896	Congestion Control in IP/TCP Internetworks
RFC 903	Reverse Address Resolution Protocol
RFC 904	Exterior Gateway Protocol Formal Specification
RFC 919	Broadcasting Internet Datagrams

(continued)

Table 7. Standards Supported by Version 13.10 *(continued)*

Standard	Description
RFC 922	Broadcasting Internet Datagrams in Subnets
RFC 925	Multi-LAN Address Resolution
RFC 950	Internet Standard Subnetting Procedure
RFC 951	Bootstrap Protocol
RFC 959	File Transfer Protocol
RFC 994	Protocol for Providing the Connectionless-mode Network Service
RFC 1009	Requirements for Internet Gateways
RFC 1027	Using ARP to Implement Transparent Subnet Gateways
RFC 1042	Transmission of IP over IEEE/802 Networks
RFC 1058	Routing Information Protocol
RFC 1075	Distance Vector Multicast Routing Protocol (DVMRP)
RFC 1076	Redefinition of Managed Objects for IEEE 802.3 Repeater Devices (AN hubs only)
RFC 1079	Telnet Terminal Speed Option
RFC 1084	BOOTP Vendor Information Extensions
RFC 1091	Telnet Terminal-Type Option
RFC 1108	Security Options for the Internet Protocol
RFC 1112	Host Extensions for IP Multicasting Appendix I. Internet Group Management Protocol
RFC 1116	Telnet Line-mode Option
RFC 1139	Echo Function for ISO 8473
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157	Simple Network Management Protocol (SNMP)
RFC 1163	BGP-2 (obsoleted by RFC 1267)
RFC 1164	Application of BGP in the Internet
RFC 1166	Internet Numbers
RFC 1188	Proposed Standard for the Transmission of IP over FDDI
RFC 1191	Path MTU Discovery
RFC 1209	Transmission of IP Datagrams over SMDS
RFC 1212	Concise MIB Definitions

(continued)

Table 7. Standards Supported by Version 13.10 *(continued)*

Standard	Description
RFC 1213	MIB for Network Management of TCP/IP-based Internets
RFC 1267	Border Gateway Protocol 3 (BGP-3; obsoletes RFC 1163)
RFC 1293	Inverse ARP for Frame Relay
RFC 1294	Multiprotocol Interconnect over Frame Relay (obsoleted by RFC 1490)
RFC 1304	Definition of Managed Objects for the SIP Interface Type
RFC 1305	Network Time Protocol
RFC 1315	Management Information Base for Frame Relay DTEs
RFC 1321	MDS Digest Algorithm
RFC 1323	TCP Extensions for High Performance
RFC 1331	Point-to-Point Protocol (PPP; obsoleted by RFC 1661)
RFC 1332	PPP Internet Protocol Control Protocol (IPCP)
RFC 1333	PPP Link Quality Monitoring (obsoleted by RFC 1989)
RFC 1334	PPP Authentication Protocols
RFC 1350	The TFTP Protocol (Revision 2)
RFC 1356	Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode
RFC 1376	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1377	OSI over PPP
RFC 1378	PPP AppleTalk Control Protocol (ATCP)
RFC 1390	Transmission of IP and ARP over FDDI Networks
RFC 1403	BGP OSPF Interaction
RFC 1434	Data Link Switching: Switch-to-Switch Protocol
RFC 1483	Multiprotocol Encapsulation over ATM AAL5
RFC 1490	Multiprotocol Interconnect over Frame Relay (obsoletes RFC 1294)
RFC 1541	Dynamic Host Configuration Protocol
RFC 1552	The PPP Internetwork Packet Exchange Control Protocol (IPXCP)
RFC 1577	Classical IP and ARP over ATM
RFC 1583	OSPF Version 2
RFC 1585	MOSPF: Analysis and Experience
RFC 1634	Novell IPX over Various WAN Media (IPXWAN)

(continued)

Table 7. Standards Supported by Version 13.10 *(continued)*

Standard	Description
RFC 1638	PPP Bridging Control Protocol (BCP)
RFC 1654	Border Gateway Protocol 4 (BGP-4; obsoleted by RFC 1771)
RFC 1661	Point-to-Point Protocol (PPP; obsoletes RFC 1331)
RFC 1662	PPP in HDLC-like Framing
RFC 1717	PPP Multilink Protocol (MP; obsoleted by RFC 1990)
RFC 1755	Signaling Support for IP over ATM
RFC 1757	Remote Network Monitoring Management Information Base (RMON), for AN, ANH, and ARN equipped with data collection module only
RFC 1762	PPP Banyan VINES Control Protocol (BVCP)
RFC 1763	PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1764	PPP XNS IDP Control Protocol (XNSCP)
RFC 1771	Border Gateway Protocol 4 (BGP-4; obsoletes RFC 1654)
RFC 1795	Data Link Switching: Switch-to-Switch Protocol, Version 1
RFC 1819	Internet Stream Protocol, Version 2
RFC 1974	PPP Stac LZS Compression Protocol
RFC 1989	PPP Link Quality Monitoring (obsoletes RFC 1333)
RFC 1990	PPP Multilink Protocol (MP; obsoletes RFC 1717)
RFC 2068	HTTP Version 1.1
RFC 2069	An extension to HTTP: Digest Access Authentication
RFC 2104	HMAC: Keyed-Hashing for Message Authentication
RFC 2138	Remote Authentication Dial In User Service (RADIUS)
RFC 2139	RADIUS Accounting
RFC 2166	Data Link Switching, Version 2.0, Enhancements
RFC 2205	Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification
RFC 2338	Virtual Router Redundancy Protocol
VINES 4.11	BayRS works with the Banyan VINES 4.11 standard. BayRS Version 8.10 (and later) also supports VINES 5.50 sequenced routing.

Flash Memory Cards Supported

You use Personal Computer Memory Card International Association (PCMCIA) flash memory cards to store the software image and the configuration files in Bay Networks routers. Software images for BayRS 13.10 require 8 or 16 MB flash cards; however, you can store configuration files on 4 MB flash cards.

Table 8 lists the flash memory cards approved for use.

Table 8. Approved Flash Memory Cards

Size	Vendor	Part Number
4 MB	Advanced Micro Devices (AMD)	AMC004CFLKA-150
	AMP	797262-3
		797263-2
	Centennial	FL04M-20-11119
		FL04M-20-11138
	Epson	HWB401BNX2
	IBM	IBM1700400D1DA-25
	Intel	IMC004FLSAQ1381
8 MB	AMD	AMC008CFLKA-150
		AMC008CFLKA-200
		AMC008CFLKA-250
		AMC008DFLKA-150
		AMC008DFLKA-200
		AMC008DFLKA-250
	Centennial	FL08M-25-11119-01
		FL08M-15-11119-01
		FL08M-20-11138
		FL08M-20-11119-01
	Epson	HWB801BNX0
	Intel	IMC008FLSP/Q1422
	Centennial (Strata-Flash)	FL08-20-11736-J5-61
16 MB	Epson	HWB161BNX2
	Centennial (Strata-Flash)	FL16-20-11736-J5-61